Best Practices for DoD Purchase Card Online System (PCOLS)

Thomas Kik
Program Manager, Defense Logistics Agency Logistics Information Service

A Winning Hand: Solutions, Savings and Sustainability with GSA SmartPay

The 13th Annual GSA SmartPay Training Conference, Las Vegas

Best Practices

House Rules

To ensure the best possible learning experience for participants, please adhere to the following house rules:

- Turn cell phones and pagers to vibrate
- Hold questions to end of session
- Ensure your participant badge is scanned to receive CLP credits
  - For each course
  - Must leave room and re-enter
- Take advantage of opportunities to provide feedback
  - Please select the Citi Q&A icon on any Citi PC at the conference
  - Answers to be emailed after the conference within 60 days

PCOLS Best Practices

Agenda

- **Sign-on and Referral System (SRS)**
- **Enterprise Monitoring and Management of Accounts (EMMA)**
- **Authorization, Issuance and Maintenance (AIM)**
- **Defense Eligibility Enrollment Reporting System (DEERS) and User Maintenance Portal (UMP)**
- **PCOLS Reporting**
- **Data Mining and Risk Assessment (DM/RA)**
- **Help and Support**

PCOLS Best Practices

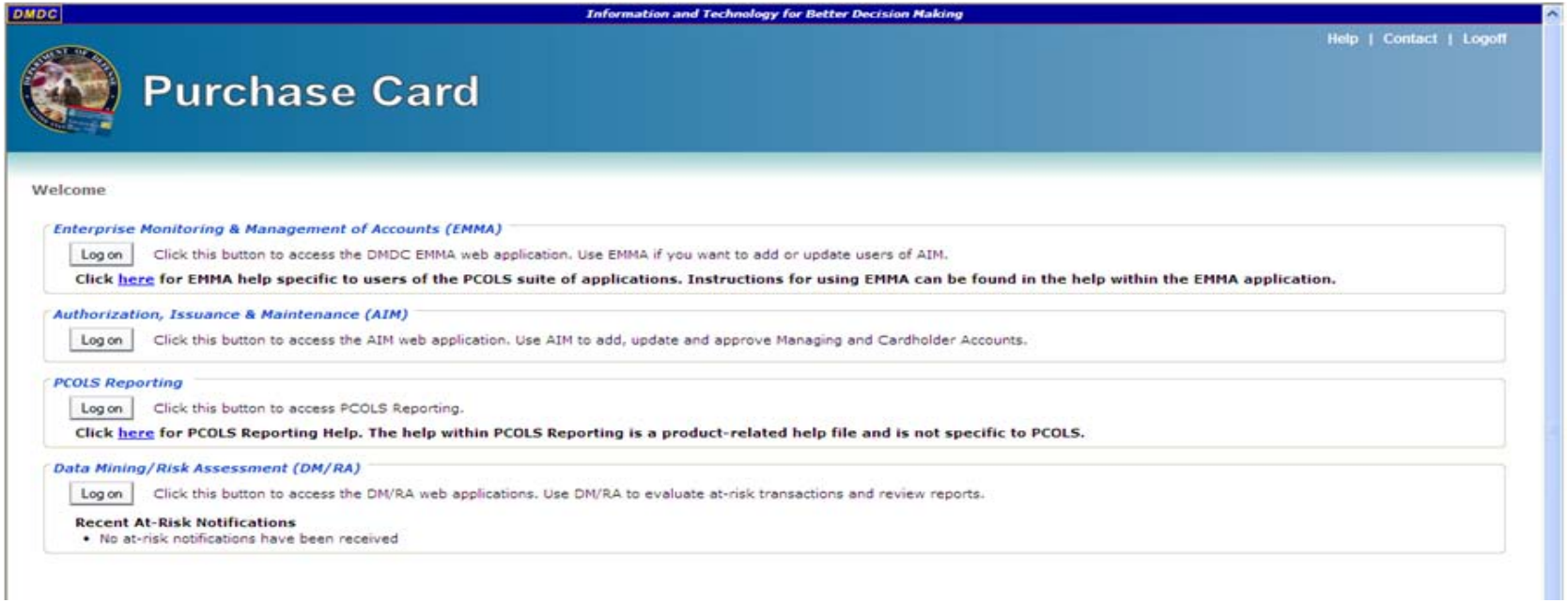
1. Sign-On and Referral System (SRS)

SRS

PCOLS consists of Enterprise Monitoring and Management of Accounts (EMMA), Authorization, Issuance and Maintenance (AIM), Data Mining and Risk Assessment (DM/RA) and PCOLS Reporting. Each of these applications is accessed through the PCOLS Sign-on and Referral System (SRS) application

When accessing any of the PCOLS applications be sure to use the Single Sign-on SRS URL:

https://pki.dmdc.osd.mil/appj/pcols-web/


DMDC
Information and Technology for Better Decision Making
Help | Contact | Logoff
Purchase Card
Welcome
Enterprise Monitoring & Management of Accounts (EMMA)
Log on
Click this button to access the DMDC EMMA web application. Use EMMA if you want to add or update users of AIM.
Click here for EMMA help specific to users of the PCOLS suite of applications. Instructions for using EMMA can be found in the help within the EMMA application.
Authorization, Issuance & Maintenance (AIM)
Log on
Click this button to access the AIM web application. Use AIM to add, update and approve Managing and Cardholder Accounts.
PCOLS Reporting
Log on
Click this button to access PCOLS Reporting.
Click here for PCOLS Reporting Help. The help within PCOLS Reporting is a product-related help file and is not specific to PCOLS.
Data Mining/Risk Assessment (DM/RA)
Log on
Click this button to access the DM/RA web applications. Use DM/RA to evaluate at-risk transactions and review reports.
Recent At-Risk Notifications
No at-risk notifications have been received

PCOLS Best Practices

2. Enterprise Monitoring and Management of Accounts (EMMA)

EMMA

EMMA is a web application used to create organizational hierarchies and to provision users into roles in these organizations. Organizations and users in roles must be established for use in the other applications of PCOLS i.e. AIM, DM/RA and PCOLS Reporting.

DOs

- Utilize the POOL concept when possible. This allows for a much easier transition when users leave a location and must be replaced
- Provision one role beneath your own
- Remove an old user once you have received confirmation that the newly provisioned user has redeemed their token(important for roles that have only one user provisioned)
- Use the PCOLS Reporting Provisioning Status Report to check the status of pending and redeemed EMMA tokens
- Reference the most current EMMA User Manual (EMMA 4.1)

DON'Ts

- Remove a user from their role before adding a replacement in the role
- Remove a user from their role because the email address is incorrect after the token has been redeemed. Have the individual update their email address in UMP
- Attempt to provision a cardholder. Cardholders do not have a role or access to EMMA

3. Authorization, Issuance and Maintenance (AIM)

AIM

The AIM application is a workflow tool used to perform various Purchase Card Program **account authorization** and **maintenance functions** . AIM draws from hierarchies recorded in EMMA. Users provisioned in EMMA will be available to select when setting up and maintaining accounts in AIM

DOs

- ▲ Verify the user profile has been set up correctly
- ▲ Check the POC list on an account to verify all users are correct before initiating a maintenance action
- ▲ Verify Primary A/BOs and Cardholders have accurate and complete work address and phone number listed before final approval and submission to the bank by the A/OPC.
- ▲ Log in under the correct role
- ▲ "Terminate Workflow" in "Accounts in Progress" if the workflow on the account cannot be completed due to an incorrect user
- ▲ Verify the Lines of Accounting (LOA) are correct
- ▲ Reference the most current AIM User Manual (AIM 2.2)

DON'Ts

- ▼ Update an account at the bank and then perform the same maintenance action in AIM.
- ▼ Submit a new managing or cardholder account to the bank if the account holders' address is missing or invalid
- ▼ Initiate a second maintenance action if the account is currently pending action in a workflow
- ▼ Forward task assignment notification emails to individuals that need to complete a task, but are not listed in the original email
- ▼ Use incorrect combinations of MCCs
- ▼ Migrate accounts into AIM under the incorrect organization
- ▼ Leave accounts in a status that have users missing from the POC list

PCOLS Best Practices

4. DEERS and UMP

DEERS and UMP

Defense Eligibility Enrollment Reporting System (DEERS)
https://www.dmdc.osd.mil/appj/address/
User Maintenance Portal (UMP)
https://www.dmdc.osd.mil/ump/

- **Work Address**
  - Verify work address is present in Profile Tab of AIM
  - Add or update work address through link in Profile Tab or by accessing DEERS application
- **Phone Number**
  - Only enter a valid US phone number (10 digits)
  - No international or DSNs (International DSNs are acceptable)
  - This field is optional
  - Bank submission failure will result if the phone number is not 10 digits
- **Email Address**
  - Verify email address is correct in Profile Tab of AIM
  - Add or update email address through link in Profile Tab or by accessing the UMP application

PCOLS Best Practices

5. PCOLS Reporting

PCOLS Reporting Users

	Account Status	Annual Review of Managing Accounts	Approving/Billing Official	Conflict of Interest	Provisioning Status	Purchase Card	Training Due	Workflow Aging
Resource Manager						x		
PCPMO Representative	x	x	x	x	x	x	x	x
Acquisition Executive Agent	x	x	x	x	x	x	x	x
HCA Agent	x	x	x	x	x	x	x	x
High-Level A/OPC Supervisor	x	x	x	x	x	x	x	x
A/OPC Supervisor	x	x	x	x	x	x	x	x
A/OPC	x	x	x	x	x	x	x	x
A/BO Supervisor		x	x	x	x	x	x	x
A/BO						x		x
Cardholders Supervisor						x	x	x

PCOLS Reporting

- Reports can be generated only for organizations in which a user is associated
- When creating reports, many of the visible functions in the application are product-related and are not PCOLS-specific. It is recommended that you not click buttons other than those specified in the instructions
- The PCOLS data base will be updated during the 2:00am to 5:00am Eastern Standard Time (EST) system unavailability window; therefore, current data in all reports will not be available until the next business day. During this time the PCOLS Reporting log on button will be disabled

PCOLS Best Practices

6. DM/RA

DM/RA

The Data Mining (DM) component of the DM/RA application provides a single user interface for users to access DoD purchase card transaction data. DM programmatically reviews 100% of transactions. Each transaction is assigned a score by the Risk Predictive Model.

DOs

- Verify that the A/BO has been assigned to the managing account in AIM. They will be unable access the case reviews until they are assigned
- Log in under the correct role/organization when locating a flagged transaction.
- Use the Total Business Reporting (TBR) information in the flagged transaction email to verify what role to use (if the user is assigned to multiple managing accounts)
- Click on the compatibility view button if an error message “select a case disposition” appears when saving a case (for users with IE8)

DON’Ts

- Forward flagged transaction emails to A/BO’s requesting they take action if they are not listed in the To: line of the original flagged transaction email
- Click the “Create” button next to a transaction unless you would like to self initiate a case review. Only transactions highlighted in blue with a “View” button are flagged and required to be reviewed
- Have multiple browsers open for the application at the same time. This can cause the user to be locked out of a case review

DM/RA (cont'd)

The Data Mining (DM) component of the DM/RA application provides a single user interface for users to access DoD purchase card transaction data. DM programmatically reviews 100% of transactions. Each transaction is assigned a score by the Risk Predictive Model.

DOs

- To disposition a case review as valid must select "Yes" for question 8. "Was green procurement considered?"
- Use the CTRL button in question 9 to select the minimum required source documentation items
- Keep track of high risk transaction emails that need to have independent reviews to be completed (Only applies to A/OPC role)*

DON'Ts

- Leave flagged transactions un-reviewed. If unable to complete a case, designate it as "Under A/BO Review" within 10 business days
- Try to log into DM/RA from previous emails. Use the SRS URL. This screen will show the last ten at-risk notifications that were created
- Disregard older flagged transactions that need to be reviewed. There will be no emails generated for transactions flagged prior to A/BO assignment to the Managing Account in AIM

DM/RA

The **Risk Assessment (RA)** application is a powerful tool that uses internal controls and measures coupled with the results from the DM application to quantify and report the inherent risk of DoD organizations' purchase card program. All this information is displayed through organizational dashboards in the RA application.

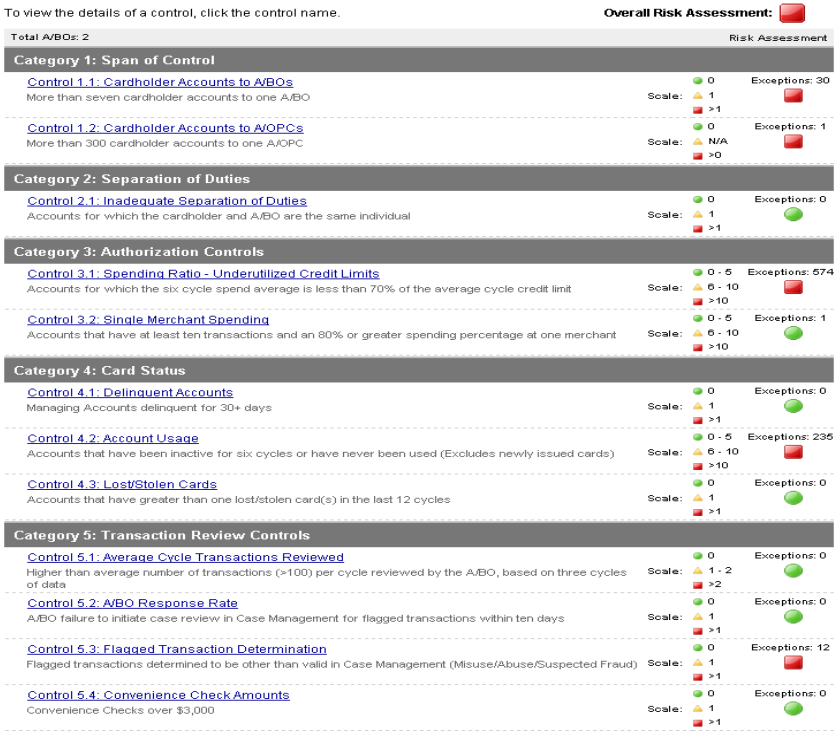
Elements of the Dashboard
Dashboards assess risk for each individual control based on specific thresholds. Also, based on the risk assessment of each of the twelve controls, an overall risk assessment is calculated for the user's hierarchical level

The RA Application assesses risk as either:

= Low (green)

= Medium (yellow)

= High (red)


To view the details of a control, click the control name.
Overall Risk Assessment:
Total A/BOs: 2
Risk Assessment
Category 1: Span of Control
Control 1.1: Cardholder Accounts to A/BOs
More than seven cardholder accounts to one A/BO
Scale: 0 1 >1
Exceptions: 30
Control 1.2: Cardholder Accounts to A/OPCs
More than 300 cardholder accounts to one A/OPC
Scale: 0 N/A >0
Exceptions: 1
Category 2: Separation of Duties
Control 2.1: Inadequate Separation of Duties
Accounts for which the cardholder and A/BO are the same individual
Scale: 0 1 >1
Exceptions: 0
Category 3: Authorization Controls
Control 3.1: Spending Ratio - Underutilized Credit Limits
Accounts for which the six cycle spend average is less than 70% of the average cycle credit limit
Scale: 0 - 5 6 - 10 >10
Exceptions: 574
Control 3.2: Single Merchant Spending
Accounts that have at least ten transactions and an 80% or greater spending percentage at one merchant
Scale: 0 - 5 6 - 10 >10
Exceptions: 1
Category 4: Card Status
Control 4.1: Delinquent Accounts
Managing Accounts delinquent for 30+ days
Scale: 0 1 >1
Exceptions: 0
Control 4.2: Account Usage
Accounts that have been inactive for six cycles or have never been used (Excludes newly issued cards)
Scale: 0 - 5 6 - 10 >10
Exceptions: 235
Control 4.3: Lost/Stolen Cards
Accounts that have greater than one lost/stolen card(s) in the last 12 cycles
Scale: 0 1 >1
Exceptions: 0
Category 5: Transaction Review Controls
Control 5.1: Average Cycle Transactions Reviewed
Higher than average number of transactions (>100) per cycle reviewed by the A/BO, based on three cycles of data
Scale: 0 1 - 2 >2
Exceptions: 0
Control 5.2: A/BO Response Rate
A/BO failure to initiate case review in Case Management for flagged transactions within ten days
Scale: 0 1 >1
Exceptions: 0
Control 5.3: Flagged Transaction Determination
Flagged transactions determined to be other than valid in Case Management (Misuse/Abuse/Suspected Fraud)
Scale: 0 1 >1
Exceptions: 12
Control 5.4: Convenience Check Amounts
Convenience Checks over $3,000
Scale: 0 1 >1
Exceptions: 0

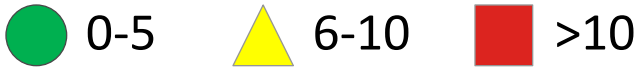
Utilize the drill-down capability allows users to see more details on each control and understand the data that supports the exceptions and the risk assessment

DM/RA

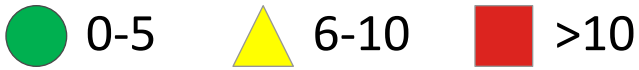
The RA application assesses risk using 12 controls. Each of the twelve controls falls under one of five categories: Span of Control, Separation of Duties, Authorization Controls, Card Status and Transaction Review Controls.

DOs

- Maintain a greater than 70% of the average credit limit within the six cycles on accounts (3.1: Spending Ratio-Underutilized Credit Limits)



- Have accounts with greater than 10 transactions maintain a less than 80% spending limit to one merchant (3.2:Single Merchant Spending Limit



DON'Ts

- Have more than 7 cardholder accounts under one A/BO (1.1: Cardholder Accounts to A/BOs)

- Establish more that 300 Cardholder accounts under one A/OPC (1.2: Cardholder Accounts to A/OPCs)

- Set up accounts that have the Cardholder and A/BO as the same individual (2.1: Inadequate Separation of Duties)

RA (cont'd)

The RA application assesses risk using 12 controls. Each of the twelve controls falls under one of five categories: Span of Control, Separation of Duties, Authorization Controls, Card Status and Transaction Review Controls.

DOs

- Keep the average number of transactions on an account under 100, based on three cycles of data (5.1: Average Cycle Transactions Reviewed)

- Initiate case reviews on flagged transactions within 10 days (5.2: A/BO Response Rate)

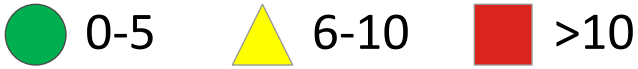
- Monitor the amount of flagged transactions determined not valid (5.3: Flagged Transaction Determination)

- Monitor the number of lost/stolen cards greater that one in the last 12 cycles (4.3: Lost/Stolen Cards)

DON'Ts

- Have Managing Accounts delinquent for 30+ days (4.1: Delinquent Accounts)

- Keep accounts open that have been inactive for six cycles or have never been used. This excludes newly issue cards 60 days from the end of the billing cycle (4.2: Account Usage)



- Issue convenience checks over $3,000 (5.4:Convenience Check Amounts)

PCOLS Best Practices

7. Help and Support

Help and Support

PCOLS Help Desk

Phone: 800-376-7783, com 269-961-7307, or DSN 661-7307

Email: dlacontactcenter@dla.mil

Operation Hours: 24x7

PCOLS DAU Continuous Learning Module CLG005

https://learn.dau.mil/html/clc/Clc1.jsp

Contains: Role-Based Training for PCOLS

PCOLS Website at DAU Acquisition Community Connection (ACC)

http://acc.dau.mil/CommunityBrowser.aspx?id=213561 or

PCOLS Website at DLA Logistics Information Service

http://www.logisticsinformationservice.dla.mil/PCOLS/

Contains: Frequently Asked Questions (FAQs)

System User Manuals (EMMA, AIM, DM/RA, REPORTING)

DEERS Address Update and User Maintenance Portal Links

Various Training Aids

Best Practices

Thomas Kik

Best Practices

Reminders

- Thank you for attending!
- Visit the Citibank Welcome Center
  - Level 3 Foyer - West
  - National Industries for the Blind will have a display of products
  - Conference Slide Show – come see yourself shine!
- Visit the Citibank One-on-One Lab – Lido Room 3101 A/B
- Visit the Citibank Mini Sessions – Lido Room 3001 A/B
- Citi Q&A Link – Tell us your thoughts

Terms & Disclosures

IRS Circular 230 Disclosure: Citigroup Inc. and its affiliates do not provide tax or legal advice. Any discussion of tax matters in these materials (i) is not intended or written to be used, and cannot be used or relied upon, by you for the purpose of avoiding any tax penalties and (ii) may have been written in connection with the "promotion or marketing" of any transaction contemplated hereby ("Transaction"). Accordingly, you should seek advice based on your particular circumstances from an independent tax advisor.

Any terms set forth herein are intended for discussion purposes only and are subject to the final terms as set forth in separate definitive written agreements. This presentation is not a commitment to lend, syndicate a financing, underwrite or purchase securities, or commit capital nor does it obligate us to enter into such a commitment. Nor are we acting in any other capacity as a fiduciary to you. By accepting this presentation, subject to applicable law or regulation, you agree to keep confidential the existence of and proposed terms for any Transaction.

Prior to entering into any Transaction, you should determine, without reliance upon us or our affiliates, the economic risks and merits (and independently determine that you are able to assume these risks) as well as the legal, tax and accounting characterizations and consequences of any such Transaction. In this regard, by accepting this presentation, you acknowledge that (a) we are not in the business of providing (and you are not relying on us for) legal, tax or accounting advice, (b) there may be legal, tax or accounting risks associated with any Transaction, (c) you should receive (and rely on) separate and qualified legal, tax and accounting advice and (d) you should apprise senior management in your organization as to such legal, tax and accounting advice (and any risks associated with any Transaction) and our disclaimer as to these matters. By acceptance of these materials, you and we hereby agree that from the commencement of discussions with respect to any Transaction, and notwithstanding any other provision in this presentation, we hereby confirm that no participant in any Transaction shall be limited from disclosing the U.S. tax treatment or U.S. tax structure of such Transaction.

We are required to obtain, verify and record certain information that identifies each entity that enters into a formal business relationship with us. We will ask for your complete name, street address, and taxpayer ID number. We may also request corporate formation documents, or other forms of identification, to verify information provided.

Any prices or levels contained herein are preliminary and indicative only and do not represent bids or offers. These indications are provided solely for your information and consideration, are subject to change at any time without notice and are not intended as a solicitation with respect to the purchase or sale of any instrument. The information contained in this presentation may include results of analyses from a quantitative model which represent potential future events that may or may not be realized, and is not a complete analysis of every material fact representing any product. Any estimates included herein constitute our judgment as of the date hereof represent potential future events that may or may not be realized, and is not a complete analysis of every material fact representing any product. Any estimates included herein constitute our judgment as of the date hereof and are subject to change without any notice. We and/or our affiliates may make a market in these instruments for our customers and for our own account. Accordingly, we may have a position in any such instrument at any time.

Although this material may contain publicly available information about Citi corporate bond research, fixed income strategy or economic and market analysis, Citi policy (i) prohibits employees from offering, directly or indirectly, a favorable or negative research opinion or offering to change an opinion as consideration or inducement for the receipt of business or for compensation and (ii) prohibits analysts from being compensated for specific recommendations or views contained in research reports. So as to reduce the potential for conflicts of interest, as well as to reduce any appearance of conflicts of interest, Citi has enacted policies and procedures designed to limit communications between its investment banking and research personnel to specifically prescribed circumstances.

© 2011 Citibank, N.A. All rights reserved. Citi, Citi Arc Design, CitiDirect, Citimanager, Citibank Custom Reporting System, Citibank Electronic Reporting System, are trademarks and service marks of Citigroup Inc. or its affiliates and are used and registered throughout the world.

In January 2007, Citi released a Climate Change Position Statement, the first US financial institution to do so. As a sustainability leader in the financial sector, Citi has taken concrete steps to address this important issue of climate change by: (a) targeting $50 billion over 10 years to address global climate change: includes significant increases in investment and financing of alternative energy, clean technology, and other carbon-emission reduction activities; (b) committing to reduce GHG emissions of all Citi owned and leased properties around the world by 10% by 2011; (c) purchasing more than 52,000 MWh of green (carbon neutral) power for our operations in 2006; (d) creating Sustainable Development Investments (SDI) that makes private equity investments in renewable energy and clean technologies; (e) providing lending and investing services to clients for renewable energy development and projects; (f) producing equity research related to climate issues that helps to inform investors on risks and opportunities associated with the issue; and (g) engaging with a broad range of stakeholders on the issue of climate change to help advance understanding and solutions.
Citi works with its clients in greenhouse gas intensive industries to evaluate emerging risks from climate change and, where appropriate, to mitigate those risks.

©2011 Citibank, N.A. All rights reserved. Citi, Citi and Arc Design and CitiDirect are trademarks and service marks of Citigroup Inc., used and registered throughout the world.